REMARKS

On December 7, 2004, the examiner, Mr. Massimiliano Poletto, Mr. Robert Nazzal and the undersigned conducted a telephonic interview. Discussed were claim 1 and the distinctions between the clustered gateway and the control center.

Applicant pointed out that regarding claim 1, that claim 1 claimed a monitoring device including a plurality of probe devices and a cluster head, and that claim 3 claimed ••• a control center. Applicant pointed out these features in the figures and specification, noting that the probe devices of claim 1 were disposed to collect statistical information on packets sent between the network and the data center. Applicant offered to amend claim 1 and correspondingly the other claims to clarify this feature.

Applicant also pointed out that the references applied by the examiner, namely by US Patent Application 2002/0035683 A1, US Patent Application 2002/0032774 A1 and US Patent Application 2002/0032880 A1 showed a gateway and a control center, but the gateway of these references did not have the features of a plurality of probe devices and a cluster head, as claimed in claim 1. No agreement was reached.

Before addressing the rejections, it might be helpful to review for the examiner distinctions between the clustered monitor and the control center concepts.

The clustered monitor is advantageously used to detect and determine packets that are part of attacks on data centers with multiple links to a network or handle traffic levels beyond what single monitor device can handle. Probes in the cluster can share information with the cluster head, so that the clustered monitor can determine if an attack is underway involving the data center. Probes in a clustered monitor can query and push information to or from the clustered monitor. A full set of detection mechanisms as well as responses to attacks can exist at the clustered monitor enabling the clustered monitor to be a stand-alone monitor. Alternatively, the arrangement allows the clustered monitor to be coupled to a control center via a redundant network.

Thus, the clustered arrangement can allow higher-bandwidth and more in-depth analysis than a non-clustered solution, whereas a control center arrangement (as taught in the references) provide a central view of the entire network, potentially across many clustered devices.

The examiner rejected claims 1-32 under 35 U.S.C. 102 (e), as being anticipated by US Patent Application 2002/0035683 A1, US Patent Application 2002/0032774 A1 and US Patent Application 2002/0032880 A1.

Claims 1-32 have been amended to clarify distinctions over these references. As amended, Claim 1 calls for a monitoring device ••• comprising a plurality of probe devices that are disposed to collect statistical information on packets that are sent over links that couple the network to the data center and a cluster head coupled to each of the plurality of probe devices, the cluster head receiving collected statistical information from the probe devices and determining from the collected information whether the data center is under a denial of service attack.

In response to Applicant's prior Reply, the examiner contends that "the two networks in which the inventions are to be used, '974 and the prior art are structurally the (sic) identical. Therefore, an identical device is inherently capable of performing the same functions, regardless of what the devices are labeled."

Applicant has now clearly shown that these features are not shown in the publications and that these features are claimed structural differences. The publications describe a gateway and data collectors. The gateway and data collectors however do not have the features of a plurality of probe devices disposed to collect statistical information on packets sent over links that couple the network to the data center and a cluster head coupled to each of the plurality of probe devices.

In the publications, the data collectors are coupled, via a redundant network, to a central control center. Instant claim 3 recites that the cluster head further includes a communication process that communicates statistics collected in the probe devices with a control center.

The control center is distinct from the cluster head in the instant claims and application and that of the publications, and therefore the publications neither describe nor suggest the

invention of claim 1 or claim 3, at least for the reasons that the publications do not suggest a plurality of probe devices disposed to collect statistical information on packets sent over links that couple the network to the data center and a cluster head coupled to each of the plurality of probe devices.

Claims 4-7 add distinguishing features, as discussed of record. Claim 8 and its dependent claims and claim 15 and its dependent claims also recite "links that couple the network to the data center" such as in claim 8 which recites monitoring network traffic through probes that are disposed to monitor packets over links that couple the victim data center and the network, and thus, clearly distinguish these claims from the references.

Claim 17 distinguishes by reciting a monitoring device ... comprising a device that collects statistical information on packets that are sent between the network and the data center over a plurality of links, and that produces statistical information from network traffic over the plurality of links to determine from the statistical information whether the data center is under a denial of service attack.

Claim 22 distinguishes by reciting a method of thwarting denial of service attacks on a victim data center by monitoring network traffic over a plurality of links between the victim data center and the network and communicating data over a redundant network to a control center.

The examiner rejected claims 1, 4, 8-10, 13 and 16 under 35 U.S.C. 101 as same type double patenting or alternatively under the judicially created doctrine of obviousness type double patenting over claims 1, 3-4, 6-8, 12-15, 17, and 26-27 of US Patent Application 2002/0035683 A1.

Claims 1, 4, 8-10, 13 and 16 do not claim the same invention as claims 1, 3-4, 6-8, 12-15, 17, and 26-27 of US Patent Application 2002/0035683 A1. For instance, claim 8 of the instant application recites:

> 8.   A method of thwarting denial of service attacks on a
> victim data center coupled to a network comprises:
> monitoring network traffic through probes that are disposed
> to monitor packets over links that couple the victim data center and
> the network; and

communicating data from the probes, over a dedicated
network, to a cluster head device.

Claim 1 of the '683 published application recites:

1. A method of thwarting denial of service attacks on a
victim data center coupled to a network comprises:
monitoring network traffic through monitors disposed at a
plurality of points in the network; and
communicating data from the monitors, over a hardened,
redundant network, to a central controller.

Claim 8 of the instant application requires that monitoring occurs through probes that are
disposed to monitor links between the victim data center and the network and that the probes
communicate data to a cluster head device. These features of claim 8 are not recited in Claim 1
of the '683 application. Thus, clearly claims 8 and 1 do not claim the same invention. The
monitors are disposed in different points, and in one case the monitors communicate with a
cluster head whereas in the case of claim 1 of the '683 application they communicate with the
central controller. A central controller is described in both applications and is not the same
element as a cluster head which is shown in FIG. 3 of the instant case but is not shown in the
'683 application. Similar arguments apply for the other claims.

The rejection of Claims 1, 4, 8-10, 13 and 16 over claims 1, 3-4, 6-8, 12-15, 17, and 26-
27 of US Patent Application 2002/0035683 A1 under judicially created doctrine of obviousness
type double patenting rejection is also improper. Again using claim 8 of the instant application
and claim 1 of the '683 published application, as illustrative, claim 8 of the instant application
requires that monitoring occurs through probes that are disposed to collect information ••• on
links between the victim data center and the network and that the probes communicate data to a
cluster head device. Claim 1 of the '683 application requires that monitoring uses monitors
disposed at a plurality of points in the network and that the monitors communicate data to a
central controller.

Claims 8 and 1 claim inventions that are non-obvious and patentably distinct from one
another. The monitors are disposed in different points in the different claims and the probes

Applicant : Massimiliano Antonio Poletto et al.   Attorney's Docket No.: 12221-011001
Serial No. : 10/062,974
Filed   : January 31, 2002
Page   : 12 of 12

communicate with a cluster head in claim 8 of the instant case, whereas in claim 1 of the '683 application they communicate with the central controller. A central controller is described in both applications and is not the same element as a cluster head, which is shown in FIG. 3 of the instant case but is not shown in the '683 application. Similar arguments apply for the other claims.

Consequently, the double patenting rejection under 35 U.S.C. 101 and the obviousness type double patenting rejection are improper.

Applicant has enclosed an Information Disclosure Statement that cites references that has come to the attention of the applicant. The references cited in this IDS taken with the cited and applied or not applied references neither describe nor suggest Applicant's invention.

The Reply accompanies a Request for Continued Examination. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 12 20 04

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

20991382.doc